IN THE CLAIMS

1. (Currently Amended) A method ~~for transporting encrypted media,~~ comprising:

receiving a call request over a packet switched network at a first gateway that is located between the packet switched network and a circuit switched network;

comparing a phone number included in the call request with entries in a local dial plan located at the first gateway;

sending one or more signals from the first gateway to a source endpoint when the phone number included in the request matches one of the entries in the local dial plan, the signals directing the source endpoint to encrypt media packets for the requested call using a protocol for encrypting real-time media;

determining whether a remote second gateway that is located on a transfer path for the encrypted media packets that are received according to the signals and that is located between the circuit switched network and the same or another packet switched network is configured for end-to-end secure transport when the requested call is to be transferred using the circuit switched network;

establishing an Internet Protocol (IP) link over the circuit switched network extending from the first gateway to the second gateway when the second gateway is configured for end-to-end secure transport; and

transferring the encrypted media packets over the established IP link.

~~receiving a request to transport encrypted Internet Protocol (IP) media packets over a circuit switched network;~~

~~establishing an IP link over the circuit switched network;~~

~~receiving encrypted IP media packets corresponding to the request, the encrypted IP media packets having encrypted layer four transport layer headers and layer three network layer headers;~~

~~replacing the existing layer three network layer headers with locally generated layer three network layer headers independently of the encrypted layer four transport layer headers and without replacing the encrypted layer four headers such that encryption protecting the layer four headers and corresponding encompassed payloads is preserved and not locally decrypted; and~~

~~transporting the revised encrypted IP media packets over the IP link established over the circuit switched network~~.

2. (Currently Amended) A method according to claim 1 further including:

decrypting the encrypted media packets locally at the first gateway when the remote second gateway is not configured for end-to-end secure transport;

formatting media included in the encrypted media packets into a Packet Switched Telephone Network (PSTN) format when the remote second gateway is not configured for end-to-end secure transport; and

transferring the formatted media over the circuit switched network for re-encryption at the remote second gateway.

~~including establishing a data channel over the circuit switched network and using a Point to Point Protocol over the data channel to establish the IP link~~.

3. (Currently Amended) The method according to claim 1 including establishing a data channel over the circuit switched network and using a Point to Point Protocol over the data channel to establish the IP link ~~claim 2 including establishing the data channel over an Integrated Services Digital Network (ISDN) channel of a Public Services Telephone Network~~.

4. (Currently Amended) A method according to claim 3 including establishing the data channel over an Integrated Services Digital Network (ISDN) channel of the circuit switched network ~~claim 1 including transporting the revised encrypted IP media packets over a packet switched network without decrypting or decoding the media that includes voice data~~.

5. (Cancelled)

6. (Cancelled)

7. (Currently Amended) A method according to claim 1 including:

authenticating the second gateway ~~an ingress device associated with the IP media packets~~;

sending a first encrypted key associated with the source ~~a first~~ endpoint over the circuit switched network to the authenticated second gateway ~~ingress device~~;

receiving a second encrypted key over the circuit switched network from the authenticated second gateway ~~ingress device associated with a second endpoint~~;

decrypting the second key and forwarding the decrypted second key over the [[a]] packet switched network to the source ~~first~~ endpoint;

encrypting the media packets at the source ~~first~~ endpoint using the first key according to the signals, the encrypted media packets directed to a destination ~~the second~~ endpoint ~~using the first key~~; and

decrypting ~~the revised encrypted~~ IP ~~media~~ packets received at the source ~~first~~ endpoint ~~received from the second endpoint~~ using the second key.

8. (Currently Amended) A method according to claim 1 including encrypting the [[IP]] media packets only once at the source ~~a first sending~~ endpoint and decrypting the [[IP]] media packets only once at a receiving second endpoint.

9. (Currently Amended) A method according to claim 1 including:

encrypting the [[IP]] media packets using a Secure Real-time Transport Protocol (SRTP);

establishing a Point to Point Protocol (PPP) connection over an Integrated Services Digital Network(ISDN) channel in the circuit switched network; and

sending the SRTP encrypted IP media packets over the PPP connection.

10. (Currently Amended) A network processing device, comprising:

a processor configured to establish ~~a connection~~ an Internet Protocol (IP) link for transferring encrypted IP packet payloads over a circuit switched network, the IP link extending across the circuit switched network and between the network processing device and a remote gateway that is located between a packet switched network and the same or another circuit switched network ~~two endpoints that extends over an Internet Protocol (IP) network and a circuit switched network~~[[,]];

the processor forwarding packets having an encrypted IP packet payload ~~between the two endpoints~~ over the IP link without decrypting the encrypted IP packet payload ~~when transferred between the IP network and circuit switched network~~.

11. (Cancelled)

12. (Currently Amended) A network processing device according to claim 10 wherein the processor compresses the forwarded packets using ~~selects a first codec when forwarding other IP packet payloads that are decrypted for transport over a PSTN connection in the circuit switched network and selects a second~~ a first data compression codec having greater data compression capability than ~~with higher compression than the first codec when~~ a second data compression codec used by the processor for other traffic that is ~~the encrypted IP packet payload is not~~ decrypted before forwarding ~~and transported~~ over a data link in the circuit switched network.

13. (Currently Amended) A network processing device according to claim 10 including a memory containing a dial plan for identifying phone numbers that can be transferred between the packet switched [[IP]] network and the circuit switched network without decrypting the encrypted IP packet payload.

14. (Currently Amended) A network processing device according to claim 10 including memory for storing a shared key shared with the remote gateway ~~an ingress device located at an ingress side of the IP network~~, the processor receiving a first key from a first endpoint, encrypting the first key using the shared key and sending the encrypted first key to the remote gateway ~~ingress device~~.

15. (Currently Amended) A network processing device according to claim 14 wherein the processor receives a second encrypted key from the remote gateway ~~ingress device~~, the processor decrypting the second encrypted key using the shared key and then forwarding the second decrypted key to the first endpoint.

16. (Currently Amended) A network processing device according to claim 10 wherein the processor conducts a Point to Point Protocol over an Integrated Services Digital Network (ISDN) channel for establishing the [[an]] IP link over the circuit switched network and then forwards Secure Real-time Transport Protocol (SRTP) encrypted IP packet payloads over the IP link.

17. (Currently Amended) A method for transporting encrypted media, comprising:

receiving a call request over a packet switched network at a first gateway that is located between the packet switched network and a circuit switched network;

determining whether a second on-path gateway includes a capability for end-to-end secure real-time transport in response to receiving the call request;

transferring the encrypted media packets over an Internet Protocol (IP) connection that traverses the circuit switched network and extends between the first and second gateways when the second gateway includes the capability for end-to-end secure real-time transport; and

converting the received encrypted media packets to a Publicly Switched Telephone Network (PSTN) format for transmission across a different connection that also traverses the circuit switched network when the second gateway does not include the capability for end-to-end secure real-time transport.

~~receiving call requests from endpoints;~~

~~identifying call requests requiring media encryption;~~

~~directing endpoints for the identified call requests to encrypt media using an Internet Protocol(IP) encryption protocol;~~

~~identifying the call requests that also require connections over a Public Services Telephone Network(PSTN);~~

~~establishing data links over the PSTN for the identified call requests;~~

~~receiving encrypted packets corresponding to the IP encrypted media from the endpoints for the identified call requests, the encrypted packets having encryption on a transport layer four header that does not encrypt a lower layer header;~~

~~formatting the lower layer header while preserving the encryption on the transport layer four header; and~~

~~forwarding the formatted IP encrypted media over the data links established on the PSTN.~~

18. (Currently Amended) The method according to claim 17 including:

authenticating the call request with the second gateway ~~identified call requests with ingress gateways~~;

conducting Point-to-Point Protocol (PPP) sessions with the second gateway ~~ingress gateways~~ when the second gateway ~~ingress gateways~~ is [[are]] authenticated; and

exchanging encryption keys with the second gateway ~~ingress gateways~~ during the PPP session.

19. (Currently Amended) The method according to claim 18 including:

encrypting the encryption keys using keys shared with the second gateway ~~ingress gateways~~; and

sending the encrypted encryption keys ~~key~~ to the second gateway ~~ingress gateways~~.

20. (Currently Amended) An apparatus, comprising:

one or more processors; and

a memory coupled to the processors comprising instructions executable by the processors, the processors operable when executing the instructions to:

receive media packets over a packet switched network at a first gateway that is located between the packet switched network and a circuit switched network, the media packets encrypted with a protocol for encrypting real-time media;

determine whether a remote second gateway is configured for end-to-end secure real-time transport before establishing an Internet Protocol (IP) connection over the circuit switched network and to the remote second gateway; and

transfer the encrypted media packets over the established IP connection when the remote second gateway is configured for end-to-end secure real-time transport.

~~receive packets over a packet switched network, the packets having first and second headers excluded from encryption for a third header and a payload;~~

~~format the first and second headers without decrypting the encryption for the third header and the payload such that the third header and the payload remain encrypted during transfer between the endpoints;~~

~~establish a connection over a circuit switched network to a remote network device; and~~

~~send the packets having the formatted first and second headers and the encrypted third header and payload on the connection over the circuit switched network.~~

21. (Currently Amended) The apparatus of claim 20 wherein the processors are further operable to:

compare a phone number included in a call request for the media packets with a dial plan; and

send a signal that causes a source endpoint for the media packets to encrypt the media packets with the protocol when the phone number corresponds with the dial plan.

~~wherein the first header is according to the Internet Protocol (IP), the second header is according to the User Datagram Protocol (UDP) and the third header is according to a secure real-time protocol~~.

22. (Currently Amended) The apparatus of claim 20 wherein the encrypted media packets include ~~payload includes~~ voice data such that the voice data is securely transported across both the circuit switched network and the packet switched network without intermediary decryption.

23. (Currently Amended) The network processing device of claim 10 wherein the processor is further configured to:

identify one or more Internet Protocol (IP) ~~network layer~~ headers included in the packets;

remove the IP ~~network layer~~ headers while preserving encryption on one or more Secure Real-time Transport Protocol (SRTP) ~~transport layer~~ headers and a corresponding payload;

locally generate one or more new IP ~~network layer~~ headers;

attach the generated IP headers to the encrypted SRTP ~~transport layer~~ headers and the encrypted corresponding payload; and

forward the packets having the locally generated IP headers, the encrypted SRTP ~~transport layer~~ headers and the encrypted corresponding payload over the IP connection.

24. (Currently Amended) The network processing device according to claim 10 where the processor is further configured to:

receive a pre-configuring out-of-band communication that provides a secret that is shared with the [[a]] remote gateway ~~located between the circuit switched network and the packet switched network~~;

receive a first key sent from a calling endpoint and usable for decrypting the encrypted IP packet payload;

encrypt the first key using the secret;

send the encrypted first key to the remote gateway;

receive a second key that corresponds to a value stored on a called endpoint and that is encrypted by the remote gateway using the secret;

decrypt the received encrypted second key using the secret; and

send the decrypted second key to the calling endpoint.

25. (New) A system, comprising:

first and second network devices, at least one of the first and second network devices located between a packet switched network and a circuit switched network;

the first network device to receive encrypted media packets from a source endpoint; and

the first network device to transfer the encrypted media packets over a connection extending through the circuit switched network and extending to the second network device for forwarding to a destination endpoint without decryption by the second network device;

wherein the encrypted media packets are sent from the source endpoint to the destination endpoint over a call path that extends across both the packet switched network and the circuit switched network without decryption by any intermediary devices located on the call path.

26. (New) The system of claim 25 wherein the encrypted media packets represent video to be played out at the destination endpoint.

27. (New) The system of claim 25 wherein both the first and second network devices are gateways located between the circuit switched network and the packet switched network.

28. (New) The system of claim 25 further comprising:

a third network device located between the circuit switched network and the packet switched network;

the first network device to determine whether the third network device is capable of an End-to-End Secure Real-time Transport Protocol (EE-SRTP) protocol; and

the first network device to decrypt packetized information for local conversion into a Publicly Switched Telephone Network (PSTN) format when the third network device is not capable of the EE-SRTP protocol; and

the first network device to transfer the decrypted and converted information over the circuit switched network to the third network device for forwarding to a destination address location in the packet switched network.

29. (New) The system of claim 28 wherein the first network device is configured to determine whether the third network device is capable of an End-to-End Secure Real-time Transport Protocol (EE-SRTP) protocol by accessing a dial plan stored locally on the first network device.